FreeBSD Administration - Feature #588

pfSense DMZ Trap Door Rule

03/31/2015 10:37 AM - Daniel Curtis

Status:	Closed	**Start date:**	03/31/2015
Priority:	High	**Due date:**	
Assignee:	Daniel Curtis	**% Done:**	100%
Category:	Firewall/Router	**Estimated time:**	0.50 hour
Target version:	pfSense 2.2	**Spent time:**	1.50 hour

Description

One of the rules I need for my firewall is to allow established connections from my LAN to my DMZ, but block any newly created connection from my DMZ to my LAN. This is to prevent any potential compromise of my DMZ from spilling over into my LAN.

- Luckily pfSense can handle this with a simple rule. Start by going to Firewall -> Rules and then select the **DMZ** tab.
- Next create a new rule by clicking on **[+]** and use the following settings.
  - Action: **Block**
  - Interface: **DMZ**
  - Protocol: **TCP/UDP**
  - Source: **DMZ net**
  - Destination: **LAN net**
  - Destination Port Range: **Any**
  - TCP Flags Set: **SYN[X]**
  - TCP Flags Out Of: **SYN[X] ACK[X]**

History

#1 - 03/31/2015 10:38 AM - Daniel Curtis

- Subject changed from DMZ Trap Door Rule to pfSense DMZ Trap Door Rule

#2 - 03/31/2015 10:40 AM - Daniel Curtis

- Description updated

- % Done changed from 0 to 50

#3 - 03/31/2015 10:42 AM - Daniel Curtis

- Description updated

#4 - 04/01/2015 11:27 AM - Daniel Curtis

- Status changed from New to Resolved

- % Done changed from 50 to 100

#5 - 04/11/2015 01:20 PM - Daniel Curtis

- Status changed from Resolved to Closed